SEARCH & SEIZURE – CELL PHONE

Riley v. California / U.S. v. Wurie, --- U.S. --- (2014)
Decided June 25, 2014

FACTS: In the first case, Riley was stopped in Los Angeles police for expired registration tags, it was then learned that his license was also suspended. His car was impounded and searched pursuant to the agency's inventory policy. Two handguns were found, and Riley was then arrested for the concealed weapons. Riley was searched and items associated with gang activity were found. The officer seized Riley's smart phone from his pocket, "accessed information on the phone and noticed that some words (presumably in text messages or a contacts list)" also suggested involvement in gang activity.

Two hours later, a detective specializing in gangs "further examined the contents of the phone," looking for potential evidence such as photos or videos. He found, in particular, a photo of Riley standing in front of a vehicle suspected of being involved in a recent shooting. Riley was charged in that shooting, with enhancements for committing the crimes to benefit a criminal gang. Riley moved to suppress the evidence obtained from the phone, which was denied. Riley was convicted and the California appellate courts affirmed his conviction.

In the second case, Wurie was observed by Boston police during routine surveillance making an "apparent drug sale from a car." He was arrested, taken to the station and two phones were seized. One, a "flip phone," was 'repeatedly receiving calls" from a number identified on the phone's external screen as "my home." They opened it and saw, as the phone's wallpaper, a woman and a baby. They were able to track the number to an apartment building. There, they saw that Wurie's name was on the mailbox and through a window, saw a woman who appeared to be the one in the photo. They secured the apartment, obtained a search warrant and eventually found drugs, weapons and cash. Wurie, a felon, was charged with distribution of drugs and possession of the firearms. He moved for suppression and was denied. He was convicted but upon appeal, the First Circuit Court of Appeals reversed his conviction.

In both cases certiorari was requested and the U.S. Supreme Court granted review.

ISSUE: May a cell phone be routinely searched incident to arrest?

HOLDING: No

DISCUSSION: The Court noted that both cases "concern the reasonableness of a warrantless search incident to a lawful arrest." In Weeks v. U.S., the Court had ruled that it had long been recognized that it was permissible to "search the person of the accused when legally arrested to discover the seize the fruits or evidences of crime."[1]

[1] 232 U.S. 383 (1914)

Although usually called an exception, in fact, the Court agreed, that was "something of a misnomer," since "warrantless searches incident to arrest occur with far greater frequency than searches conducted pursuant to a warrant." Since that time, the scope of such searches has been debated, with three specific cases illustrating the parameters of the argument.

In Chimel v. California, the Court "laid the groundwork for most of the existing search incident to arrest doctrine."[2] In Chimel, the Court agreed it was reasonable to search the person to remove any weapons or items that might be used to aid in an escape. It further noted it was "entirely reasonable for the arresting officer to search for and seize any evidence … to prevent its concealment or destruction." In U.S. v. Robinson, the court applied the rule to the contents of a cigarette package found on the person of an arrested subject and ruled that a "custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification."[3] That was clarified in U.S. v. Chadwick, however, which ruled that a locked footlocker in the possession of the arrested subject could not be searched incident to arrest.[4] Finally, in Arizona v. Gant, the Court emphasized that "concerns for officer safety and evidence preservation underlie the search incident to arrest exception."[5]

Moving to the specific issue of "how the search incident to arrest doctrine applies to modern cell phones," the Court noted that they "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." Although such phones were unknown just ten years ago, now, it noted "a significant majority of American adults now own such phones." Even though Wurie's was a "less sophisticated" phone than Riley's, that model had only "been around for less than 15 years." Both were based on technology that was "nearly inconceivable" when Chimel and Robinson were decided.

The Court noted that balancing tests created in earlier cases simply did not apply 'with respect to digital content on cell phones" and found little to no risk of harm or destruction of evidence "when the search is of digital data." Although an arrested subject loses a great deal of privacy rights, "cell phones … place vast quantities of personal information literally in the hands of individuals."

Further, the Court agreed:

> Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. Law enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not

[2] 395 U. S. 752 (1969),
[3] 414 U. S. 218 (1973),
[4] 433 U. S. 1, 15 (1977)
[5] 556 U.S.332 (2009); A further exception allowed under Gant, searching for evidence related to the crime of arrest, stemmed from "circumstances unique to the vehicle context."

> be used as a weapon—say, to determine whether there is a razor blade hidden between the phone and its case. Once an officer has secured a phone and eliminated any potential physical threats, however, data on the phone can endanger no one.

Although the Government in both cases suggested that there might be indirect ways that searching the phone might protect officers, the Court found that there had been no proof in either case that such "concerns are based on actual experience.' To the extent that a particular case might have such an issue arise, the Court found it to be "better addressed" by treating it as a specifically articulated exigency based upon specific facts.

In both cases, the Government focused primarily, however, on the destruction of evidence prong. In both cases, it was argued that:

> … that information on a cell phone may nevertheless be vulnerable to two types of evidence destruction unique to digital data—remote wiping and data encryption. Remote wiping occurs when a phone, connected to a wireless network, receives a signal that erases stored data. This can happen when a third party sends a remote signal or when a phone is preprogrammed to delete data upon entering or leaving certain geographic areas (so-called "geofencing").

In addition, it argued that encryption is a security feature in some phones, used along with passwords/codes. When locked, the information is inaccessible unless the password is known. In the case of remote wiping, the primary concern is not with the arrested subject, who cannot access the phone, but with third parties. However, the Court noted that it had been given no evidence that "either problem is prevalent" – as it had been provided with "only a couple of anecdotal examples of remote wiping triggered by an arrest.' With respect to searching a phone before the password triggers the phone to lock down, the Court noted that law enforcement officers are "very unlikely to come upon such a phone in an unlocked state because most phones lock at the touch of a button or, as a default, after some very short period of inactivity."

> Moreover, in situations in which an arrest might trigger a remote-wipe attempt or an officer discovers an unlocked phone, it is not clear that the ability to conduct a warrantless search would make much of a difference. The need to effect the arrest, secure the scene, and tend to other pressing matters means that law enforcement officers may well not be able to turn their attention to a cell phone right away. Cell phone data would be vulnerable to remote wiping from the time an individual anticipates arrest to the time any eventual search of the phone is completed, which might be at the station house hours later. Likewise, an officer who seizes a phone in an unlocked state might not be able to begin his search in the short time remaining before the phone locks and data becomes encrypted.

The Court noted that remote wiping can be prevented by disconnecting the phone from the network, by turning it off, removing the battery or placing the phone in a Faraday bag to isolate it from signals. While this is not necessarily a "complete answer to the

problem," it is, at least a reasonable response, already in use by some law enforcement agencies. The Court agreed, however that if there truly is an exigent circumstances, especially one with life-or-death consequences, "they may be able to rely on exigent circumstances to search the phone immediately."[6] Or, if the phone is unlocked, secure it so that it does not automatically lock.[7] The theoretical threat of a remote wipe of the data, alone, is not sufficient, however, to be considered an exigent circumstances, particularly since it can be, as a rule, prevented by alternative means.

The Court noted that although an arrested subject has "diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely." Despite the assertion that a search of a cell phone, in the context of an arrest, is "materially indistinguishable" from the search of other items in their possession.

The Court continued:

> Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers. One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only narrow intrusion on privacy. Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so. And if they did, they would have to drag behind them a trunk of the sort held to require a search warrant in Chadwick, rather than a container the size of the cigarette package in Robinson.

In addition, a cell phone can contain "many distinct types of information" that together can be used to reconstruct "the sum of an individual's life." The Court contrasted a note with a person's phone number to a "record of all … communications" – and in some cases, the content of that communications, with that same individual, as might be found on a cell phone. Normally, a person would not carry about "sensitive personal information" every day, but now, that is done routinely. The Court noted that the vast majority of adults 'keep on their person a digital record" of their lives, from the "mundane to the intimate." Not only in quantity is it different, but also in quality – for example, an Internet browsing history, historic location data, various apps that might suggest a person's private life.

In U.S. v. Kirschenblatt, it was observed that : it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for

[6] Missouri v. McNeely, 133 S.Ct. 1552 (2013)
[7] See Illinois v. McArthur. 531 U.S. 326 (2001).

everything which may incriminate him."[8] However, "If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is."

To further complicate matters, a cell phone may be used to access a wealth of data located elsewhere, in what is called "cloud computing." In fact, it may not even be readily known whether a particular piece of data is one the phone itself … or located elsewhere and simply being access through the phone. Arguing that such data would be access with would be analogous to "finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house."

The Court noted that agencies should, of course have protocols, but that "the Founders did not fight a Revolution to gain the right to government agency protocols." All of the options argued before the court were found to be unfeasible and unacceptable, The Court emphasized. However, that it was not holding that a cell phone is immune from search, only that a warrant will generally be required prior to a search, unless another recognized exigent circumstance applies.

The Court concluded:

> We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost.
>
> …
>
> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life," The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.

The Court reversed the judgment in Riley and affirmed the judgment in Wurie.

Full Text of Opinion: **http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf**

[8] 16 F.2d 202 (2nd Cir. 1926).